ALERTA: IDENTIFICACIÓN DE VARIANTE MIKEY.130442 (03/DICIEMBRE/2021)

VARIAS SOLUCIONES DE ANTIVIRUS HAN DETECTADO LA PRESENCIA DE LA AMENAZA MIKEY.130442, EL MISMO AFECTA A EQUIPOS CON ARQUITECTURA DE 64 BITS EN SISTEMA OPERATIVO WINDOWS 10

Introducción

En noviembre de 2021, diferentes antivirus detectaron la presencia de una variante de MIKEY, cuyo nombre asignado es SenseSampleUploader.exe.

En el portal virus total, se especifica que once (11) de sesenta y cinco (65) antivirus logran detectar esta variante; la misma que presenta una firma digital *Authenticode* y características *Binarias Anómalas* de los equipos con Sistema Operativo Windows 10 y arquitectura de 64 bits como se muestra en la Figura 1.

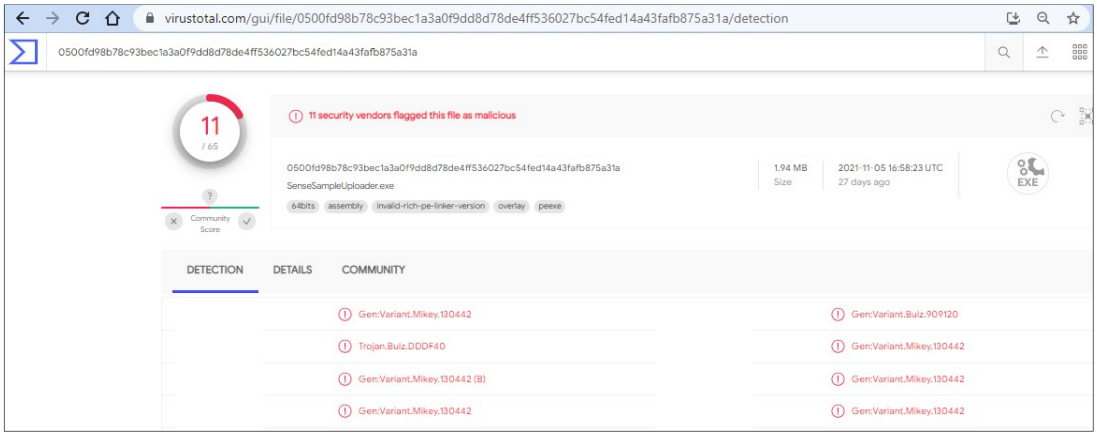

***Figura 1**: Cantidad de soluciones antivirus que detectan Mikey 130442*
***Fuente**: Sitio WEB virustotal.com*

Vector de ataque:

La distribución de Mikey puede ocurrir con la ayuda de varias técnicas de propagación de amenazas, como software pirateado, archivos adjuntos de correo electrónico corruptos y descargas falsas.

Actualmente, se está aprovechando de la actualización de Windows 10 a través de sitios WEB no oficiales.

Indicador de Compromiso:

MD5: 4a7ab0c0380b18824bf6bc36d9998c50
Tipo de variante: Gen: variant.mikey.130442
Sistema: Windows 10 arquitectura 64 bits

- *C:\Windows\WinSxS\amd64_windows-senseclient-service_31bf3856ad364e35_10.0.17134.1276_none_62a4cf99315faa39\SenseSampleUploader.exe*
- *C:\\Program Files\\Windows Defender Advanced Threat Protection\\SenseSampleUploader.exe.*

Impacto:

Mikey puede infectar ordenadores de forma silenciosa y crear varios archivos que pueden utilizarse para ejecutar operaciones amenazantes, así como para comunicarse con servidores remotos de *Command & Control (C&C)*. Los estafadores pueden usar Mikey para ejecutar una gran cantidad de acciones dañinas, como descargar amenazas adicionales, convertir la computadora infectada como parte de una *botnet*, obtener acceso ilícito a los datos del usuario, entre otros.

Recomendaciones:

- Utilizar software con licencia legal.
- Ejecutar actualizaciones de Microsoft de fuentes oficiales y confirmadas.
- Mantener siempre su computadora protegida con un software anti-malware confiable y actualizado que pueda detectar y eliminar amenazas como Mikey.
- Evitar descargar software de destinos Web no confiables. Lo mismo se aplica a los mensajes de correo electrónico, nunca abra mensajes de remitentes desconocidos, especialmente si contienen enlaces o archivos adjuntos desconocidos que no esperaba recibir.
- Reportar el HASH de los archivos en formato MD5 a su proveedor de antivirus y/o seguridad.
- Revisar en el sitio *virus total,* si la solución de antivirus utilizada brinda la protección necesaria.

Referencias

Adware Reports. (s.f.). Obtenido de https://adwareremoval.info/mikey-130442-b/

Virus Total. (s.f.). Obtenido de https://www.virustotal.com/gui/file/0500fd98b78c93bec1a3a0f9dd8d78de4ff536027bc54fed14a43fafb875a31a/detection